Signature (at least Department Head Level)

Date

Lucent Technologies
Bell Labs Innovations

DISCLOSURE OF INVENTION

THIS DESCRIPTION MAY BE SUPPLEMENTED BY ATTACHING COPIES OF RELEVANT DOCUMENTS, SUCH AS TECHNICAL MEMORANDA, PUBLISHED OR TO-BE-PUBLISHED ARTICLES, AND ENGINEERING NOTEBOOK PAGES.

(Also, if for any item there is insufficient space on the form, attach additional pages as necessary.)

Note: at least Department Head Level Approval is required.

Please Send Completed Form to:

Lourdes Chesal
(732) 949-9284
HO 3K-217
lourdes@lucent.com

SUBJECT OF SUBMISSION:

Dynamic Virtual Private Networking Technology

OBJECTIVE:

(What overall problem does the proposal solve or what purpose does it serve?)

Virtual Private Network (VPN) services are provided by Service Providers on top of their public IP networks to provide corporate (large, medium, and small enterprises) and SOHO (small office, home office) customers with secure connectivity between geographically disperse locations in lieu of connections owned or leased exclusively for a private network. Modifications to a VPN's network topology, security, service provisioning options, or Quality of Service (QoS) typically require an end-user request to their Service Provider whose personnel manually perform the VPN management. This process incurs provisioning delay, loss of revenue potential (e.g., supporting new services, applications, etc.) and is more costly to the Service Provider, and ultimately to the end-user, than automated subscriber self-provisioning. A new service approach and framework is presented here known as Dynamic VPN (D-VPN) technology. D-VPN addresses the business challenge of reducing provisioning delay and loss of revenue potential, by providing the Service Provider with technology and services to enable automated subscriber self-management of Virtual Private Network services.

With numbers from IDC (June 1999) estimating services revenues to be up to $10B by 2003 (breakdown: From a CAGR: IP VPN services 81%, VPN Equipment 42%, Management 16%), clearly widespread adoption of IP VPN technology is driving service revenues up a steep growth curve. New access mediums like wireless data are building on the IP VPN infrastructure and will place additional demands on the capabilities of the network. Thus, it is critical to reduce provisioning delay and increase revenue potential by providing the Service Provider with technology and services that enable subscriber self-management of Virtual Private Networks. D-VPN provides the framework and capability for this to happen.

Many network devices must be configured to provide VPN services. Each device is configured in its own way, either by means of a user interface resident on the device itself, or by means of a user interface implemented as part of the device's Element Management System (EMS). This use of multiple user interfaces to manage a VPN currently prevents subscriber management of VPN services. D-VPN technology facilitates subscriber management of VPN services by providing a single user interface that coordinates the automated network response to user requests. This interface interacts with a rule-based (supported by directory services and policy management) change control mechanism to configure downstream network devices. Service Provider network management personnel may also use this technology to simplify, speed the completion of, and reduce the cost of performing day-to-day VPN management tasks. Maintenance and trouble-shooting activities are thereby simplified because Service Provider technicians can use the same interface as their customers, providing a common, synchronized frame of reference for the two parties which does not exist today.

Subscriber self-management of Virtual Private Network services is further facilitated by the invention of Service Profiles, Security Profiles, and Application Profiles. A Service Profile is a novel technique used to represent and identify the topology, security, and QoS requirements of a customized, individual VPN service. A Security Profile is a novel technique used to represent and identify acceptable network activity; exceptions are regarded as security threats. An Application Profile is a novel technique used to represent and identify the connectivity, security, and QoS requirements of a network-based application, as well as information about how the application is to be accessed and billed.

Currently, Services Providers provide QoS on an IP flow statically and in one direction, for example, from the network to the end-user, if it is provided at all. A new generation of IP applications exists that have strict bi-directional QoS requirements in order to perform satisfactorily. The QoS requirements vary from application to application. Today, there is no single user interface to accommodate these dynamic QoS requirements, which vary as a function of time and application characteristics. D-VPN technology extends existing capability to provide bi-directional QoS on-demand to an IP flow from a single user interface. In addition, D-VPN technology will negotiate with the access network to modify the access network's QoS parameters, providing the access network has this capability.

Many Internet Service Providers (ISPs) and Application Service Providers (ASPs) are entering into a retailer/wholesaler relationship whereby the ISP retails ASP-provided applications to their customers. The network-based application's connectivity, security, and QoS requirements are manually provisioned in the ISP's network on a per-user, per-application basis. D-VPN technology streamlines this business arrangement by providing the capability to automatically load application-specific connectivity, security, and QoS requirements as well as billing information into the ISP's environment and to automatically configure the ISP's network to satisfy these requirements when the application is activated.

D-VPN technology combines IP bandwidth management, VPN, and Directory Enabled Networking technologies in a novel and unique way to provide a platform that extends current Service Provider network capabilities to include:

1. A single user interface for the management of VPN services. This user interface may be used by Service Provider subscribers and network management personnel.

2. On-Demand, automated management of a VPN's topology, security, and QoS parameters.
3. On-Demand, automated management of bi-directional IP QoS.
4. The ability to define and store service profiles, application profiles, and security profiles for future retrieval and use.
5. On-Demand, automated retrieval and network deployment of stored service profiles, application profiles, and security profiles in response to D-VPN service requests issued by Service Provider subscribers or network management personnel.
6. On-Demand, automated modification of network element configurations in response to a security threat.
7. The ability to automatically reject VPN and QoS configuration requests and notify the user when sufficient network resources are not available or are inconsistent with the request.
8. Automated renegotiation of access link QoS based on application or user requirements.
9. On-Demand access to network-based applications and automated network configuration to satisfy the application's connectivity, security, and QoS requirements.
10. Automated activation and deactivation of the above capabilities based on temporal and repetitive parameters.
11. Providing the above capabilities over a wireless access network.
12. The capability to provide and manage Service Level Agreements (e.g. bandwidth usage, latency, security level, and class of service) that can be managed via a Service Level Management module.
13. Automated ASP application registration with ISPs.

It is not possible to provide these capabilities using existing technology. In order to provide the above capabilities, a Service Provider augments their existing network by deploying D-VPN enabled devices at their customer premises, in their core network, and in their data centers. Current customer premises devices are augmented with D-VPN technology to become Enhanced IADs. Core network edge devices are augmented with D-VPN technology to become IP Services Aggregation Switches. The new D-VPN Manager resides in the data center and consists of an Enhanced Application Portal, an Application Registration Server, an Enhanced Policy Server, and a Directory Server. The Enhanced IADs, IP Services Aggregation Switches, and D-VPN Manager work in concert through a novel, common VPN and QoS policy management interface to extend the capabilities of current Service Provider networks to provide the capabilities listed above.

Service Provider directory schemas are currently segmented across several dimensions which necessitates the deployment of several directories and directory servers. For example, the user authentication directory is seperate from the inventory directory, which is separate from the CPE router policy directory, which is separate from the edge router policy directory, etc. The D-VPN Manager utilizes a novel directory schema that unifies these disparate directories into one common directory and directory server. This reduces the amount of equipment that Service Providers must deploy and simplifies network operations and maintenance.

Service Providers will need a functionality check-list to determine if network equipment is compatible with their D-VPN enabled networks. We have identified the minimal list of technology requirements that must be satisfied by network devices in order to be eligible for inclusion in a Service Provider's D-VPN enabled network. Devices that satisfy these requirements are classified as "D-VPN Ready."

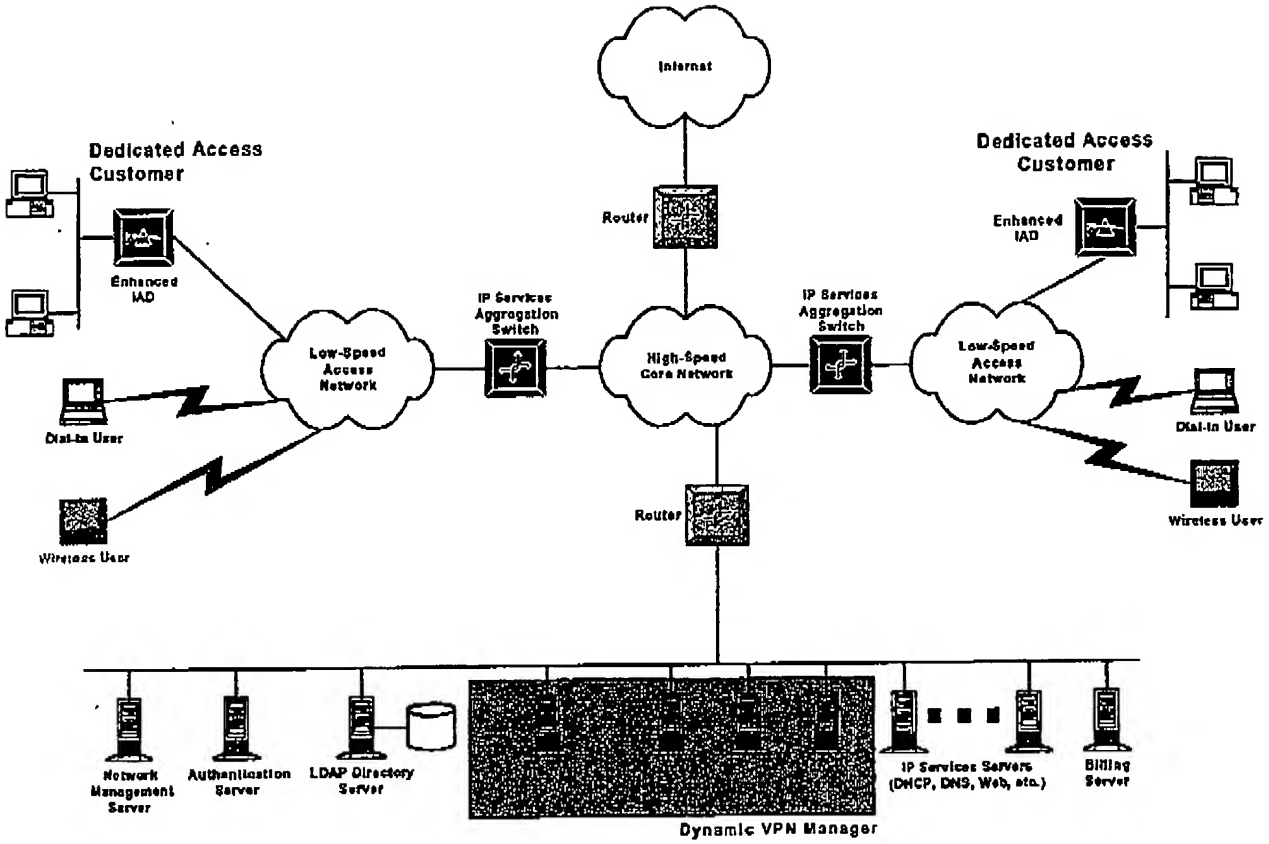
We believe that we can patent the following:

1. The novel D-VPN technology that augments existing CPE and core network devices.
2. The novel D-VPN Manager network element.
3. The novel concepts of Service Profiles, Security Profiles, and Application Profiles.
4. The above list of extended Service Provider network capabilities that are enabled by D-VPN technology.
5. The unique way in which Enhanced IADs, IP Services Aggregation Switches, and the D-VPN Manager interact to provide the capabilities listed above.
6. The newly identified set of requirements that constitute "D-VPN Ready" devices.
7. The novel VPN and QoS policy management interface that is common to all D-VPN enabled network elements.
8. The novel directory schema that results in the consolidation of Service Provider directories that were previously required to be kept separate.

BRIEF DESCRIPTION:

(1. What is it? 2. How does it operate? Rely on attachments for detailed description.)

D-VPN is a novel, distributed technology with components in a Service Provider's customer premises and in the Service Provider's core network and data centers. The following diagram depicts a Service Provider's network containing D-VPN technology and will help to understand the description that follows.



Current high-end CPE devices provide IP services such as routing, IP QoS, VPN, Encryption, and Tunneling. They also collect statistics that can be used for billing and SLA verification and management. A CPE device that satisfies these requirements is considered to be "D-VPN Ready." D-VPN technology extends the functionality of "D-VPN Ready" CPE devices to that of Enhanced IADs.

Enhanced IADs apply the above IP services plus bandwidth allocation to IP flows that are flowing away from the customer toward the ISP network. The Enhanced IAD's VPN and QoS configurations are managed by the D-VPN Manager, which coordinates the automated network response to D-VPN service requests. The Enhanced IAD receives configuration commands from the D-VPN Manager and modifies its configuration appropriately. The Enhanced IAD has the ability to verify the validity of D-VPN service requests in terms of capacity and consistency. If the request is found to be inconsistent with the current network configuration, or if the request exceeds the capacity of its access link, the Enhanced IAD rejects the configuration request.

Edge routers are currently deployed at the edge of the Service Provider core IP networks. High-end edge routers provide IP services such as routing, IP QoS, VPN, Encryption, and Tunneling. They also collect statistics that can be used for billing and SLA verification and management. An edge router that satisfies these requirements is considered to be "D-VPN Ready." D-VPN technology extends the functionality of "D-VPN Ready" edge routers to that of IP Services

Aggregation Switches. IP Services Aggregation Switches apply advanced IP services (e.g., security and QoS) plus bandwidth allocation to IP flows that are flowing towards the customer. The unique interaction between the IP Services Aggregation Switch and Enhanced IAD provide the novel, bi-directional aspect of Dynamic VPN services.

The IP Services Aggregation Switch's VPN and QoS configurations are managed by the D-VPN Manager. The IP Services Aggregation Switch receives configuration commands from the D-VPN Manager and modifies its configuration appropriately. The IP Services Aggregation Switch has the ability to verify the validity of D-VPN service requests in terms of capacity and consistency. If the request is found to be inconsistent with the current network configuration or if the request exceeds the capacity of one of its access links, the IP Services Aggregation Switch rejects the configuration request.

The IP Services Aggregation Switch also provides an endpoint for network-based services accessed by customers without Enhanced IADs. Functioning in this capacity, the IP Services Aggregation switch provides advanced IP services (e.g., security and QoS) on IP flows that are flowing towards the Service Provider's core network. This provides the capability to provide D-VPN services to wireless customers where none existed before.

The Dynamic VPN Manager is a new network element that is deployed in the Service Provider's data center to coordinate the automated network response to D-VPN service requests. The D-VPN Manager consists of the following components: (1) the Enhanced Application Portal, (2) the Application Registration Server, (3) the Policy Server, and (4) the Directory Server.

The Enhanced Application Portal extends the functionality of existing application portals in the following manner. It provides the single user interface by which Service Provider subscribers and network management personnel manage IP QoS and security, manage D-VPN services, and access network-based applications on-demand. The Enhanced Application Portal also supports temporal aspects of D-VPN services. The Enhanced Application Portal allows an end-user to attach a time duration to his/her D-VPN request. After the duration has expired, the subscriber's D-VPN service is automatically removed from the ISP's network. The end-user may also specify that the D-VPN service be made available at some time in the future and may also specify a repetitive factor to the D-VPN service. For example, an end-user may specify that a D-VPN service be made active from 6pm until midnight every Friday.

The Enhanced Application Portal interacts in a new and unique way with the Policy Server and end-user to direct the automated configuration of the network in response to end-user requests for D-VPN services. The Enhanced Application Portal authenticates the end-user. After successful authentication, the end-user may activate, deactivate, create, modify, or delete service profiles and security profiles. The Enhanced Application Portal then interacts with the Policy Server to carry out the end-user request. The Enhanced Application Portal also interfaces to a Billing Server to record the use of value-added services.

Current Policy Managers provide VPN and QoS policy management for a limited set of products, e.g., the Lucent Spring Tide LightShip Policy Manager can only manage the IPSS product line and not the Pipeline product line. The D-VPN Policy Server extends current policy management capabilities to provide a common VPN and QoS policy management interface for any D-VPN

enabled device in a Service Provider's network. Service profiles, application profiles, and security profiles are stored as policies in the Directory Server. Upon receiving a request from the Enhanced Application Portal, the Policy Server extracts these profiles from the Directory Server, converts them into commands understood by the different network elements and downloads these commands to the network elements.

Service Providers must currently deploy several directories and directory servers in their network because of the heterogeneous directory schemas defined for different network equipment products and different aspects of network functionality. For example, the user authentication directory is seperate from the edge router policy directory, which is seperate from the CPE policy directory, etc. The schema used by the D-VPN Directory Server unifies these disparate directories thus reducing the number of directories and directory servers that must be deployed by Service Providers. This results in reduced equipment costs and simplified operations for Service Providers.

The Application Registration Server replaces the current manual process used by ASPs to load applications into ISP networks. The Application Registration Server provides an interface by which authorized application managers (either ASP or Service Provider personnel) manage the application profiles stored in the Directory Server. Application profiles contain the connectivity, security, and QoS requirements of the application as well as information about how the application is to be accessed and billed. When a given application is activated by an end-user (by means of the Enhanced Application Portal), the ISP's network is automatically configured to satisfy the requirements specified in the application profile and the Billing Server is notified of this value-added service activation.

Please refer to Attachment I, "Dynamic Virtual Private Networks" by McGee, Vasireddy, Johnson, et. al. for a detailed description of D-VPN technology. This article has been submitted for publication to the *Bell Labs Technical Journal*.

COMPARISON:

(1. What similar things are already known or available? 2. What are the differences of your proposal? 3. What commercial benefits are derived from these differences?)

Lucent and our competitors (Redback, Cisco, Nortel, Shasta, Cosine, Quarry, etc.) currently have Policy Servers and web-based provisioning systems for individual network elements, or product lines of network elements. These network elements tend to be incorporated in separate portions (e.g., access, distribution, or core) of a Service Provider's network. The following table lists features related to D-VPN currently available in Lucent and competitive products.

FEATURE	ANALYSIS	VENDOR COMPLIANCE					
		LU	cisco	NT	Redback	Quarry	Cosine
TUNNELING	• All of the vendors support standard L2/L3 tunneling. [1]Redback does not have network-based IPSec. It has to be done by CPE. Redback's MPLS implementation details are somewhat sketchy.	Y	TBD	Y	N[1]	Y	Y
SECURITY	• In general, IPSec, X.509 digital certificates and network-based firewalls are supported by the vendors.	Y[2]	TBD	TBD	N[3]	Y[2]	Y[2]

	[2]Virtual Routers are implemented by Lucent, Cosine and Quarry. [3]Redback does not have the Virtual Router concept. It also does not have network-based firewalls.						
VPN ROUTING	• The vendors support the interior and exterior routing protocols, as well as multicasting. [4]Cosine emphasizes their support for IP/FR.	Y	TBD	Y	TBD	Y	TBD[4]
IP ADDRESS MANAGEMENT	[5]NAT is not supported by Redback	Y	TBD	Y	N[5]	Y	Y
NETWORK MANAGEMENT	CORBA, SNMP, LDAP and Policy-Based Networking are supported by all vendors.	Y	Y	Y	Y	Y	Y
SUBSCRIBER SELF-SERVICING	[6]In this context, Subscriber Self-Servicing simply refers to the ability to make a web-based provisioning interface available to a subscriber on a per-device basis. No vendor has a single user interface for end-to-end provisioning or the network intelligence provided by D-VPN technology.	Y[6]	TBD	Y[6]	Y[6]	Y[6]	Y[6]
ACCOUNTING	Per flow, per customer call detail records are generated by most vendors. Ability to generate micro-billing needs further investigation.	Y	TBD	Y	Y	Y	Y
QoS	[7]Redback uses PVC to implement QoS in the network.	Y	TBD	N	N[7]	Y	N

Provisioning end-to-end VPN services is currently a manual process that requires the use of many product-specific user interfaces. As can be seen from the above table, the D-VPN capabilities described in the previous sections significantly advance the art.

D-VPN technology enables end-customers to self-subscribe on-demand to intelligent IP services with the requisite QoS values. End-customers can also exploit the bandwidth elasticity in the access segment, while paying for features on a per-use basis; for example, guarantee bandwidth to IP flows, or reserve network resources for a videoconference scheduled between multiple locations. Service performance information and billing information can be viewed on-line.

Service Providers can create a new market by augmenting their existing network infrastructure with D-VPN enabled devices to provide new revenue opportunities based on enhanced service offerings. The bandwidth in the Service Provider's access network is used on an as-needed basis for these enhanced services. This, in turn, will lead to better traffic management techniques in the Service Provider network. Per-usage billing for value-added services is also supported. In addition, Service Providers will be able to realize significant equipment cost savings and operations reductions as described in the previous sections.

Equipment vendors can include D-VPN technology in all IP-based network elements that participate in traditional VPNs. Multiple customer requirements ranging from integrated voice and data devices (IADs) to data only devices are supported. Equipment vendors will also have the opportunity to develop one generic provisioning application that can be used across many product lines. We believe that this will lead to an increase in the sales of CPE as well as network equipment.

USE:

1. What is the probability of commercial use? By LUCENT? By others?

Currently, Lucent has a strategic customer (a Service Provider) who is demanding the capabilities enabled by D-VPN technology in their network architecture. There is nothing unique about this particular Service Provider, so the probability of the commercial use of D-VPN technology is very high. In addition, a demonstration is being put together to show proof of concept of this technology and associated services. It is expected that additional customers will be interested in implementing this approach to reduce costs and gain additional revenue.

A recent Yankee Group Report states that 90% of all U.S. Service Providers will have launched or were planning to launch a web-based self-servicing project by the end of 2000. Also in a survey of medium and large businesses:

- 66.67% of end-users would prefer electronic service activation.
- 60.87% of end-users would prefer electronic service changes.

2. Is it scheduled for use in a LUCENT product or service? Which one, and when?

The i-Navis product roadmap lists a future product, called i-Policy, which can utilize this technology. i-Policy is currently in the conceptualization phase of product development. It is expected that i-Policy and other products will utilize this patent along with other internal Lucent studies to develop these capabilities for their products.

3. Is this idea likely to be adopted by others outside of LUCENT? If so, why and to what extent?

This idea is likely to be adopted by others outside of Lucent. It is expected that many of Lucent's customers may be working with other vendors, including our competitors, to facilitate the types of services that are enabled by D-VPN technologies. In addition, there are many market research reports, e.g., Gartner, IDC, Yankee Group, which project the widespread adoption of these capabilities by Service Providers.

4. Is it likely to become a standard?

It is possible that the protocols by which D-VPN enabled devices communicate with each other will become standardized. This would facilitate the interoperation of D-VPN enabled devices manufactured by multiple vendors. There are advantages and disadvantages to Lucent. If Lucent rapidly standardizes our interfaces to incorporate D-VPN protocols, then we would be first to market with an end-to-end solution and be in a position to capture the initial market and drive the standardization process.

5. Do you see applications for the idea other than the one described above?)

D-VPN technology is an enabling technology. We have identified several services that can be based on this technology:

1. **On-demand IP Bandwidth Management.** Service Provider subscribers and network management personnel are able to request that a specific amount of bandwidth be provided to an IP flow across the Service Provider's access network. The Service Provider's network is automatically configured to guarantee at least the requested amount of bandwidth to the IP flow.

2. **Dynamic VPN Management.** VPN management includes the management of a VPN's topology, security, and QoS configuration. Service Provider subscribers and network management personnel are able to create, activate, modify, deactivate, and delete VPN services on demand. The ability to apply temporal and repetitive parameters is supported as well, such as specifying that a VPN service automatically be made available every Friday from 6pm-midnight. The Service Provider's network is automatically configured in response to these VPN management requests.
3. **Network-Based Application Management and Subscription.** Authorized ASP and Service Provider personnel are able to store application profiles in the Service Provider's network. Service Provider subscribers are able to select these applications and the Service Provider's network is automatically configured to provide the network-based application to the subscriber as per the application profile.
4. **Dynamic Service Provider Network Security Policy Management.** Service Provider personnel can create, activate, modify, deactivate, and delete security policies, which define acceptable network activity, on demand. The Service Provider network is automatically configured in response to these Security Policy Management requests.

We anticipate that once D-VPN technology is widely deployed, many other applications for it will be identified.

ECONOMIC IMPACT:

(1. What is the expected annual sales volume or revenue of products or services of (a) LUCENT (b) overall marketplace, to which this proposal applies, if used?)

Incorporating D-VPN technology into Lucent networking equipment would provide a solution package with quality differentiators for Lucent products. It is reasonable to assume that these quality differentiators would allow Lucent products to capture an additional 5%-10% of the VPN equipment market share.

Synergy Research Group, Inc. has identified four VPN-related network equipment categories in which Lucent competes. According to their most recent market report, in 1999 the total market revenue for all these equipment categories was $5.2 billion. A 5%-10% increase in market share would have resulted in $260 million - $520 million in increased revenue in 1999.

For the first nine months of 2000, the total market revenue of VPN-related network equipment categories in which Lucent competes was $4.6 billion. A 5%-10% increase in market share would have resulted in $230 million - $460 million over that time period for a total increased revenue of $490 million - $980 million over the 21-month period.

A recent Yankee Group Report estimates the market size for self-service solutions, software, and professional services to be:

- Year 2000: $0.75B.
- Year 2001: $1.51B.
- Year 2002: $1.98B.

In addition, Frost & Sullivan predict that revenue from VPN services will exceed $18 billion by 2004 in United States only.

As a major provider of solutions, software, and professional services to Service Providers, Lucent has the opportunity to capture a significant portion of this market with D-VPN technology. VPNs are very often considered to be a replacement for private lines to move sensitive, business-critical data. Thus, concerns about service, regarding security, performance, new services, and service-level management are even more critical. In fact, on average, a VPN will pay for itself in less than 6 months. According to a recent study in InternetWeek Magazine, the initial purchase price of VPN hardware and software to support 120 users averages between $7K to 10K. The ROI can be as short as 3-4 months.

Overall, the VPN marketplace is growing at a phenomenal rate and IP VPNs have quickly become the fundamental infrastructure for delivering next generation IP based services. This patent is important, as Lucent is a major player in the VPN market. In addition, Lucent can leverage additional equipment sales, and service support sales, to existing customers by supporting this additional framework in addition to providing new revenue generating services for the Service Provider.

FOREIGN INTEREST:
(1. In which foreign countries, if any, should we obtain a patent? Why (e.g., big market there; major competitors are based there)?)

We should obtain patents in foreign countries in which our major competitors are based; e.g., Canada (Nortel), European countries (Siemens, Alcatel).

ORIGINATORS OF THE PROPOSAL:
(Name, Dept., Room number, Ext.)

Andrew R. McGee; BL0340200; NJ7460 4G-415A; 732-332-6445

S. Rao Vasireddy; BL0340200; NJ7460 4G-409; 732-332-5118

K. Jeffrey Johnson; BL0340200; NJ7460 4G-416A; 732-949-3444

Uma Chandrashekhar; BL0340200; NJ7460 4L-450; 732-332-6852

Steven H. Richman; BL0340200; NJ7460 4G-402; 732-332-6187

Mohamed El-Sayed; BL034200A; NJ7460 4G-401A; 732-949-0407

Attachments:
(Identify the memo)

1. "Virtual Private Networks," A.R. McGee, S.R. Vasireddy, K.J. Johnson, U. Chandrashekhar, S.H. Richman, M. El-Sayed; Submitted for Publication in the April-June, 2001 Issue of the *Bell Labs Technical Journal.*

ATTACHMENTS-